Abstract

A computer system that makes it difficult to analyze the content of a calculation. A power operation unit (262) performs the following operations using the input data "a" and "b": $g_a = g^a \mod n$, $g_b = g^b \mod n$. Next, a multiplication unit (264) performs the following calculation using g_a and g_b: $g_{ab} = g_a \times g_b \mod n$. Next, a discrete logarithm calculation unit (266) calculates $c_i \mod p_i - 1$ to satisfy $g_{ab} = g^{ci} \mod p_i$ ($i = 1, 2, 3, …, k$). Next, a CRT unit (267) calculates "c" to satisfy $c_i = c \mod p_i - 1$ ($i = 1, 2, 3, …, k$) using the Chinese remainder theorem CRT.